



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/692,747	10/18/2000	Craig L. Ogg	39478/RRT/S850	7075
23363	7590	10/15/2004	EXAMINER	
CHRISTIE, PARKER & HALE, LLP PO BOX 7068 PASADENA, CA 91109-7068			HEWITT II, CALVIN L	
			ART UNIT	PAPER NUMBER
			3621	

DATE MAILED: 10/15/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/692,747

Applicant(s)

OGG ET AL.

Examiner

Calvin L Hewitt II

Art Unit

3621

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 30 July 2004.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-45 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-45 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

Status of Claims

1. Claims 1-45 have been examined.

Response to Amendment

2. The Examiner has amended claims 1, 16 and 29 to read requiring a user to re-register if the user is using a second computer to access the system. However, the Examiner has found the amendment and associated remarks insufficient for overcoming the prior art.

When analyzing claims in a pending application, the claims should be given their broadest possible interpretation (*In re Pearson*, 181 USPQ 641 (CCPA 1974)). The first limitation of claim 1 (and 29) recites "a user using one or more computers", hence the claim applies to the method or system that is implemented using "one computer". Therefore, the last limitation that is directed to a "second computer" is not applicable and does not occur if there is only one computer. Hence, in order to anticipate claim 1, the prior art need only satisfy the first limitations (see- '317, column/line 3/44-4/12; '177, column/line 17/29-18/11). Claim 16, on the other hand, recites optional language. Specifically, the Applicant's method states that a user is to re-register **if** the second computer is not the same as the first. This understanding of the claim is further supported by

the limitation that details a user logging on to a second computer implying, in light of the last limitation, that the second computer can also be the first computer. Similarly, in claims 1 and 29, the Applicant does not require the first and second computers to be physically distinct structures. Hence, a computer that exists in a different state, or a computer at a different point-in-time, meets the requirement of a "second computer". Brookner and Sudia teach such a computer. For example, Brookner discloses re-registering if the computer has satisfied certain operating conditions thus making it distinct from the users initial registration ('317, column/line 3/44-4/12), while Sudia discloses "re-keying" (i.e. re-registration) (177, column/line 17/29-18/11).

The Examiner has maintained the rejection under 102 and 103.

In order to better define the Applicant's system the Examiner refers the Applicant to pages 18-21 of the Specification where the Applicant explains how the system determines whether or not a user is to be "re-registered". More, specifically, the issuance and encryption of the HMK key (derived from a user passphrase), the storing of the HMK key, binding of the software to the registering computer, the server using the HMK to sign requests and preventing access to the user's account by determining if a user is logged on using the HMK key.

The Examiner would also like to point out to the Applicant that the although the Applicant stated in the Remarks that claim 29 had been amended, this is not reflected in the actual claims. The Examiner, therefore, is examining claim 29 as if it had been amended.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this

Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1, 2, 3, 8, 11, 13-16, 25-29, 37 and 43-45 are rejected under 35 U.S.C. 102(e) as being clearly anticipated by Brookner, U.S. Patent No. 6,041, 317.

As per claims 1, 2, 3, 8, 11, 13-16, 25-29, 37 and 43-45, Brookner teaches a postage security system, utilizing a PSD, that comprises a user using one or more computers, a secret key for identifying a first computer and registering a user, a remote server system that communicates with one or more of computers

and receives user information and a secret key for registering a user (i.e. registering a user with an online system), a user that uses said first computer for second and subsequent communications with the remote system, and stores the secret key as part of a PSD package (abstract; figures 1 and 2; column 2, lines 18-34; column 3, lines 5-12 and 44-67; column 4, lines 1-13 and 23-38).

As per claims 13-15, 26-28, 34-36 and 43-45, Brookner teach a PSD that generates postal indicia (VBI), hence, it is inherent that a VBI (e.g. postage value, ticket or voucher) is printed.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 1-45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sudia, U.S. Patent No. 6,009,177.

As per claims 1-5, 7-19, 21-31, 33-30 and 41-45, Sudia teaches a digital communications security system comprising:

- a user using one or more computers (column 1, lines 20-58; column 2, lines 55-63; column 13, lines 30-63; column 16, lines 9-34; column 21, lines 15-53)
- a secret key for identifying a first computer and registering a user
- a remote system that communicates with one or more user computers and receives user information and a secret key for registering a user (i.e. registering a user with an online system) (column/line 17/29-18/11)
- a user that uses said first computer for second and subsequent communications with the remote system (column 21, lines 15-53)
- a secret key that comprises an encrypted randomly generated hash message authentication key that is generated at the time of registration (column/line 17/50-18/11; column 25, lines 27-51)
- a secret key that comprises an encrypted randomly generated hash message authentication key for digitally signing electronic communications thereby authenticating the user, storing said key at the user computer and changing said key at periodic intervals (column 15, lines 45-58; column 17, lines 37-48 and 55-64; column 21, lines 40-54; column 41, lines 15-43)

Sudia teaches a user computer sending an encrypted secret key to the remote system that decrypts and stores the secret key (column/line 17/50-18/11).

Sudia does not explicitly recite the type of keys used by the remote system to perform such a function. However, as Sudia recites symmetric key encryption (shared key), encryption using session keys, asymmetric encryption (public/private or secret keys used for decryption/encryption or encryption/decryption), the specific methods of Diffie-Hellman, RSA, Micali, DES, etc. It would have been at least obvious for one of ordinary skill to choose any of the disclosed methods by Sudia to enable to parties to communicate cryptographically.

Limitations identifying the type of VBI used or system with which a user is registering is merely non-functional descriptive material and, non-functional descriptive material cannot render non-obvious an invention that would have been otherwise been obvious (In re Gulack, 703 F.2d 1381, 1385, 217 USPQ 401, 404 (Fed. Cir. 1983)).

Regarding postal security devices, the teachings of Sudia are broadly applied to trusted devices that comprise an embedded microprocessor, input-output interface, memory and optionally a cryptographic co-processor (column 13, lines 30-63). A PSD is an element of the set of "trusted devices" as it comprises the features identified above. In addition, PSD's print "value bearing instruments" (VBI). Therefore, it would have been obvious to one of ordinary skill to apply the teachings of Sudia to trusted devices such as PSDs.

Sudia does not explicitly recite user computers communicating with a system that is a server system. However, Sudia teaches a user first computer communicating with another user computer (column 21, lines 27-29), securing digital communications (column 2, lines 55-63) and distributed data processing systems such as those used for distributing electronic mail (column 1, lines 20-40), hence, it is at least obvious to one of ordinary skill for the user computer to communicate with the escrow agent computer system (i.e. remote system) over computer network (figures 15 and 16) such as the internet.

7. Claims 6, 20, 32, and 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sudia, U.S. Patent No. 6,009,177 in view of Ote et al., U.S. Patent No. 6,023,506.

As per claims 6, 20, 32, and 40, Sudia teaches a digital communications security system that uses encryption keys for encrypted user computer specific information such as a secret key comprising an encrypted randomly generated hash message authentication key that is generated at the time of registration (column/line 17/50-18/11; column 25, lines 27-51). However, Sudia does not explicitly recite a specific encryption method for encrypting the user computer specific information. Ote et al. teach a method for generating an encryption key using a user pass-phrase (abstract). Therefore, it would have been obvious to one of ordinary skill to combine the teachings of Sudia and Ote et al. in order to

reduce the burden on users regarding the management of encrypting information ('506, column/line 1/65-2/6).

8. Claims 9, 13-15, 26-28, 34-36 and 43-45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Brookner, U.S. Patent No. 6,041,317.

As per claims 9, Brookner teaches a postage security system, utilizing a PSD, that comprises a user using one or more computers, a secret key for identifying a first computer and registering a user, a remote server system that communicates with one or more of computers and receives user information and a secret key for registering a user (i.e. registering a user with an online system), a user that uses said first computer for second and subsequent communications with the remote system, and stores the secret key as part of a PSD package (abstract; figures 1 and 2; column 2, lines 18-34; column 3, lines 5-12 and 44-67; column 4, lines 1-13 and 23-38). Brookner doesn't explicitly recite periodically changing a secret key comprising a hash authentication message. However, Brookner teaches that keys can be "selectively updated" therefore, to one of ordinary skill, the prior art at least suggests the periodical changing of keys (column 4, lines 18-23).

As per claims 13-15, 26-28, 34-36 and 43-45, limitations identifying the type of VBI used or system with which a user is registering is merely non-functional descriptive material and, non-functional descriptive material cannot

render non-obvious an invention that would have been otherwise been obvious
(In re Gulack, 703 F.2d 1381, 1385, 217 USPQ 401, 404 (Fed. Cir. 1983).

Conclusion

9. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

10. Any inquiry concerning this communication or earlier communications from the Examiner should be directed to Calvin Loyd Hewitt II whose telephone

number is (703) 308-8057. The Examiner can normally be reached on Monday-Friday from 8:30 AM-5:00 PM.

If attempts to reach the Examiner by telephone are unsuccessful, the Examiner's supervisor, James P. Trammell, can be reached at (703) 305-9768.

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks
c/o Technology Center 2100
Washington, D.C. 20231

or faxed to:

(703) 305-7687 (for formal communications intended for entry and after-final communications),

or:

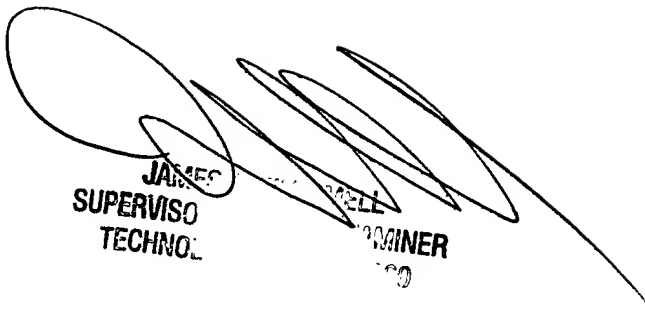
(703) 746-5532 (for informal or draft communications, please label "PROPOSED" or "DRAFT")

Hand-delivered responses should be brought to Crystal Park 5,
2451 Crystal Drive, 7th Floor Receptionist.

Any inquiry of a general nature or relating to the status of this application should be directed to the Group receptionist whose telephone number is (703) 308-1113.

Calvin Loyd Hewitt II

February 20, 2004


JAMES P. MINER
SUPERVISOR
TECHNOLOGY